Security Aspects

STUDY NOTES

- **Viruses:**
  - ❖ A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.
  - ❖ Computer virus has the tendency to make its duplicate copies on an infected system, and also spread it across every folder and damage the data of your computer system.
- **Worms:**
  - ❖ A computer worm is a type of malware that spreads copies of itself from computer to computer.
  - ❖ A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.
- **Trojan Horse:**
  - ❖ A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer.
  - ❖ Trojan Horse is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device.
  - ❖ A Trojan Horse is a code hidden in a program, that looks safe but has hidden side effects such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.
- **Spam:**
  - ❖ Email spam, also referred to as junk email or simply spam, are unsolicited messages sent in bulk by email (spamming).
  - ❖ Spam is sent in bulk for advertising purposes from an unknown sender.
- **Cookies:**
  - ❖ Cookies are small blocks of data created by a web server while a user is browsing a website and placed on the user's computer or other device by the user's web browser.
  - ❖ They are usually used to track the pages that we visit.
  - ❖ Cookies is also called web cookies, internet cookies or browser cookies.
  - ❖ Cookies are placed on the device used to access a website, and more than one cookie may be placed on a user's device during a session.
- **Adware:**
  - ❖ Adware, often called advertising-supported software.
  - ❖ Adware is an unwanted software that generates revenue for its developer by automatically throwing online advertisements up on user screen.
- **Firewall:**
  - ❖ A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
  - ❖ A firewall can be hardware, software, or both.

- **HTTP and HTTPS:**
  - ❖ Full form of HTTP is Hypertext Transfer Protocol. HTTPS stands for Hypertext Transfer Protocol Secure.
  - ❖ HTTP provides standard rules for web browsers & servers to communicate. HTTPS protocol is an extension of HTTP. That "S" in the abbreviation comes from the word Secure.
  - ❖ HTTP transfers data in plain text. HTTPS transfers data in cipher text (encrypt text).
  - ❖ HTTP is fast as compared to HTTPS. HTTPS is slow because it consumes computation power to encrypt the communication channel.
- **Hackers:**
  - ❖ A computer enthusiast, who uses his computer programming skills to intentionally access a computer without authorization is known as hacker.
  - ❖ A hacker accesses the computer without the intention of destroying data or maliciously harming the computer.
  - ❖ Hackers can also be internet security experts hired to find vulnerabilities in systems.
  - ❖ These hackers are also known as white hat hackers.
- **Crackers:**
  - ❖ Cracker is the name given to hacker who break into computers for criminal gains.
  - ❖ The general view is that, while hackers build things, crackers break things.
  - ❖ These hackers are also known as Black Hat Hackers.
- **Antivirus and their workings:**
  - ❖ Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer.
  - ❖ Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.
  - ❖ Antivirus software usually works on one of two principles: Either it scans programs and files as they enter your device and compares them to known viruses, or it scans programs already on your device, looking for any suspicious behavior.
- **Denial-of-service attack:** A Denial of service(DOS) attack is an attempt to make one or more network resources unavailable to their intended users. Examples of such attacks are:
  - ❖ **Denial of Access to information:** Corrupting, Encrypting or changing the status of information so that it is not accessible to its legitimate user.
  - ❖ **Denial of Access to application:** Forced shutting of an application as soon as the user opens it.
  - ❖ **Denial of Access to Resources:** Blocking a resource, may be a printer or scanner or USB port, of a computer from proper working.
  - ❖ **Denial of Access to a website:** Continuously sending bulk requests to a website so that it is not available to any other user.
- **Intrusion Problems:**
  - ❖ An Intrusion problem is an attempt to mischievously steal some information from someone's computer. Examples of Intrusion are: Snooping and Eavesdropping
  - ❖ The most common purposes of intrusion attacks are to: Gain unauthorised access to files, privileges, data or money.
- **Snooping:**
  - ❖ Snooping refers to gaining unauthorized access to another person's or organization's data.
  - ❖ This may be done in number of ways: By getting someone's login information by casually watching what he/she is watching, Reading the files on someone's computer in an authorized manner,
  - ❖ Using some software which keep track of the activities and data being sent or received on someone's computer.

- **Eavesdropping:**
  - ❖ Eavesdropping refers to gaining unauthorized access to another person's or organization's data while the data is on its way on the network.
  - ❖ This may be done in a number of ways:By setting up parallel telephone lines, by installing some software in the target computer, by installing some receiver which capture the data while on its way.